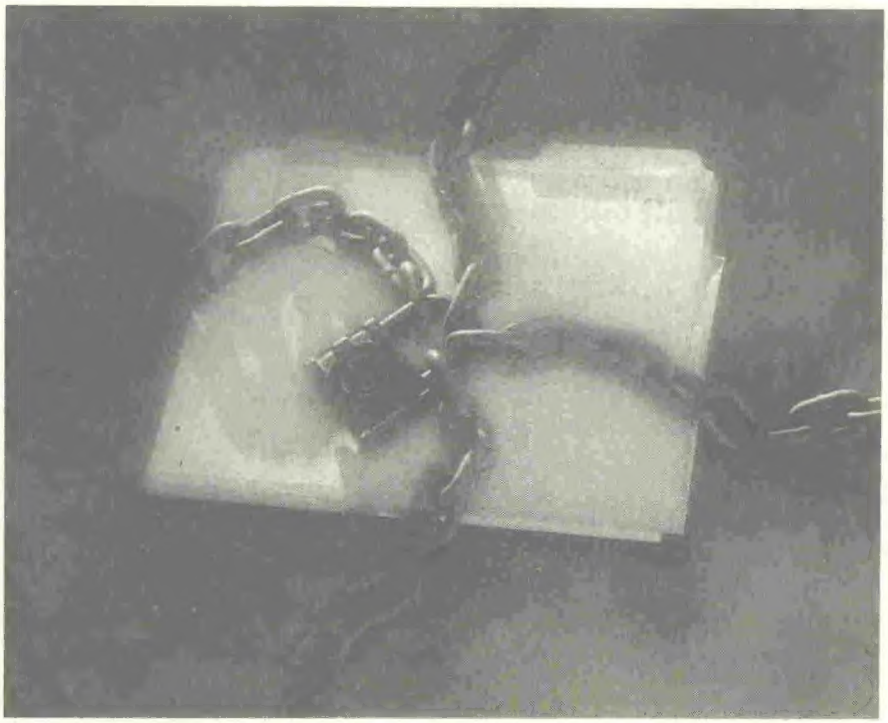
อรรถพล ตริตานนท์

ระบบสารสนเทศทางการบริหารบุคคล : ความปลอดภัยของสารสนเทศบุคคล



ความสำคัญของระบบความปลอดภัยในการบันทึกข้อมูลเพื่อขจัดความเสี่ยงในการเกิดปัญหาต่าง ๆ

ความก้าวหน้าในการพัฒนาเทคโนโลยีทางคอมพิวเตอร์ได้พัฒนาต่อไปอย่างต่อเนื่องและรวดเร็ว มีผู้ใช้จำนวนมากขึ้น ขณะเดียวกันคอมพิวเตอร์มีราคาถูกลงทุกวัน องค์กรจึงหลีกเลี่ยงต่อความก้าวหน้าในเทคโนโลยีสารสนเทศได้ยากมาก ตรงกันข้ามองค์กรต่าง ๆ กลับมาลงทุนในเทคโนโลยีสารสนเทศมากขึ้น ทำให้เกิดการตื่นตัวในการนำคอมพิวเตอร์มาปรับใช้เพิ่มประสิทธิภาพในการทำงานเพิ่มขึ้น

คงจะทราบกันดีแล้วว่าองค์กรต่าง ๆ ได้ให้ความสำคัญต่อข้อมูล (Information) เพิ่มขึ้นเป็นอย่างมาก ในอดีตเราไม่เคยคิดเลยว่าข้อมูลจะเป็นทรัพย์สิน (Resources) ที่มีค่าอย่างหนึ่งขององค์กรได้ แต่ปัจจุบันข้อมูลถือได้ว่าเป็นทรัพย์สินที่มีค่าต่อองค์กรเป็นอย่างยิ่ง จึงมี Software House หลายรายได้พยายามคิดและพัฒนาระบบสารสนเทศทางการบริหารบุคคลขึ้นมาทั้งในประเทศเองและจากต่างประเทศด้วย หากคุณได้ติดตามบทความของผมเรื่องสารสนเทศทางการบริหารบุคคลแล้ว (ฉบับเดือนพฤศจิกายน 2539) คงจะทราบข้อมูลกันมาบ้างว่าซอฟต์แวร์ในตลาดของบ้านเรายังไม่มีซอฟต์แวร์ตัวใดที่สนับสนุนการบริหารทรัพยากรบุคคลได้อย่างเต็มที่นัก มักเป็นเพียงการบันทึกข้อมูลบุคคล การบันทึกเวลาการทำงาน การจ่ายเงินเดือน ฯลฯ เท่านั้น ซึ่งสามารถอ่านเพิ่มเติมได้จากเรื่องสารสนเทศทางการบริหารบุคคล ทั้งนี้ผู้ใช้คอมพิวเตอร์ในประเทศไทยส่วนใหญ่ยังไม่ตระหนักถึงแนวทางการเก็บรักษาข้อมูลด้านบุคคลในระยะยาว ยังคงให้ความสำคัญเรื่องการจัดหาเครื่อง การจัดวางระบบ การเขียนและทดสอบโปรแกรม และการเปลี่ยนจากระบบเดิมมาใช้ระบบใหม่อยู่นั่นเอง โดยแท้ที่จริงแล้วองค์กรควรมีหน้าที่แต่เพียงจัดหาซอฟต์แวร์ทางการบริหารบุคคลมาใช้ และสอนคนให้ทำงานให้เป็นก็เป็นเรื่องหนักหนาสาหัสอยู่แล้วกว่าจะปรับเปลี่ยนทั้งกระบวนการ แนวคิด วัฒนธรรม และวิธีการทำงานจากวิธีการเดิม ๆ มาสู่วิธีการใหม่ ๆ ที่ง่ายขึ้น เป็นเหตุให้มักจะมองข้ามปัญหาที่สำคัญมากไปประการหนึ่งคือ ปัญหาเรื่องระบบความปลอดภัยของข้อมูลข่าวสารที่ได้มาว่าควรจัดการและรักษาข้อมูลเหล่านั้นอย่างไร

ดังนั้นเราจึงควรให้ความสำคัญของระบบความปลอดภัยในการบันทึกข้อมูล เพื่อลดหรือขจัดความเสี่ยงในการเกิดปัญหาต่าง ๆ ที่จะตามมาเกี่ยวกับความปลอดภัยของข้อมูล อาทิเช่น การลักลอบนำข้อมูลของผู้อื่นไปใช้ในทางที่ผิดกฎหมาย เป็นต้น ซึ่งจะก่อให้เกิดความเสียหายต่อบุคคลและองค์กรได้

ความปลอดภัยของข้อมูล

โดยทั่วไปแล้วคำว่า "ความปลอดภัย" (Security) ได้มีการใช้กันแพร่หลาย จนในบางครั้งจะมีการใช้อย่างไม่ถูกต้องมากนัก ทำให้

A.139 W.A 10

เกิดความหมายที่ผิดเพี้ยนไปบ้างแล้วแต่โอกาส โดยส่วนใหญ่แล้วคำนี้มักจะหมายถึง การเข้าไปป้องกันสิ่งที่อาจจะเกิดขึ้น หรือการทำให้ความเสี่ยงที่จะเกิดเหตุการณ์นั้น ๆ ลดลง แต่ไม่ได้หมายความว่าคุ้มครองให้ความเสี่ยงนั้น ๆ หมดไป ในชีวิตประจำวันนั้นเราสามารถสังเกตเห็นเขตปลอดภัยได้บ่อยมากตามสถานก่อสร้าง หรือตามถนนหนทางทั่ว ๆ ไป ทุกคนย่อมทราบว่าในพื้นที่นั้นมีการให้ความคุ้มครองป้องกัน โดยที่จะไม่ได้รับอันตรายใด ๆ ความปลอดภัยในด้านบุคคลก็เช่นเดียวกัน ถึงแม้จะไม่มีป้ายห้ามหรือป้ายเตือนก็ตาม เราก็ควรจะเตรียมการเพื่อป้องกันข้อมูลทางด้านบุคคลทั้งภัยจากภายในองค์กรเองและภายนอกองค์กร ด้วยเพราะข้อมูลทางด้านบุคลากรนั้นมีความสำคัญต่อองค์กรมาก

สำหรับความหมายของความปลอดภัยในทางคอมพิวเตอร์ มักจะเกี่ยวข้องกับความปลอดภัยในเรื่องของข้อมูลเป็นหลัก ผมขอใช้คำ 3 คำนี้มาใช้กับความหมายของความปลอดภัยของข้อมูลทางด้านบุคคล เพื่อให้เข้าใจถึงระดับความปลอดภัยต่าง ๆ ที่มีอยู่คือการใช้คำว่า Security, Confidentiality และ Privacy (ดังรูปที่ 1) มักมีความสับสนกัน เนื่องจากมีความเกี่ยวข้องกัน[1] อย่างใกล้ชิดจนแทบแยกกันไม่ออก โดยที่ Confidentiality มักจะเป็นเรื่องความลับ เพื่อป้องกันบุคคลที่สามรับรู้ข้อมูล ตัวอย่างที่เห็นกันได้ง่าย ๆ ก็เวลาที่เราได้รับ Payroll Slip ไงล่ะครับ ซึ่งทางฝ่ายบุคคลจะเป็นผู้ส่งให้พนักงานแต่ละคนและจะมีการแสตมป์คำว่า "Confidential" กำกับไว้เสมอ ขณะที่ Privacy จะเป็นข้อมูลเรื่องสิทธิส่วนบุคคลซึ่งจะเป็นอันตรายมากเมื่อมีคนเข้าไปใช้โดยผิดวัตถุประสงค์ เช่น ข้อมูลบุคคล ข้อมูลการสมรส ข้อมูลเกี่ยวกับโรคประจำตัว ข้อมูลประวัติการรักษา เป็นต้น ส่วน Security จะเป็นสิ่งที่จำเป็นต้องมีเพื่อเป็นการคุ้มครองป้องกันทั้งปัจเจกบุคคลและนายจ้างในการใช้ข้อมูลโดยผ่านกระบวนการต่าง ๆ ก่อนเข้าถึงข้อมูล[2] สิ่งหนึ่งที่เป็นความรับผิดชอบในการออกแบบระบบบริหารทรัพยากรบุคคล ก็คือ การป้องกันสิทธิส่วนบุคคลในส่วนของข้อมูลที่ถูกเก็บในฐานข้อมูล เมื่อเราได้ทราบความหมายของทั้งสามคำแล้ว ลองสังเกตดูซิครับว่า Privacy กับ Sucurity แตกต่างกันอย่างไร **Privacy** จะหมายถึงสิทธิส่วนบุคคลของพนักงานที่บุคคลอื่น ๆ ไม่สามารถรับรู้ได้นอกจากการยินยอม **Security** จะเป็นเพียงการป้องกันข่าวสารข้อมูลหรือทรัพยากรที่สามารถผ่านเข้าไปเก็บในคอมพิวเตอร์ โดยปกป้องมิให้ผู้ใช้ซึ่งไม่ได้รับอนุญาต เช่น คู่แข่งขัน เข้าไปเปิดใช้[3] เท่านั้น

ความปลอดภัยในการบันทึกข้อมูลบุคคล

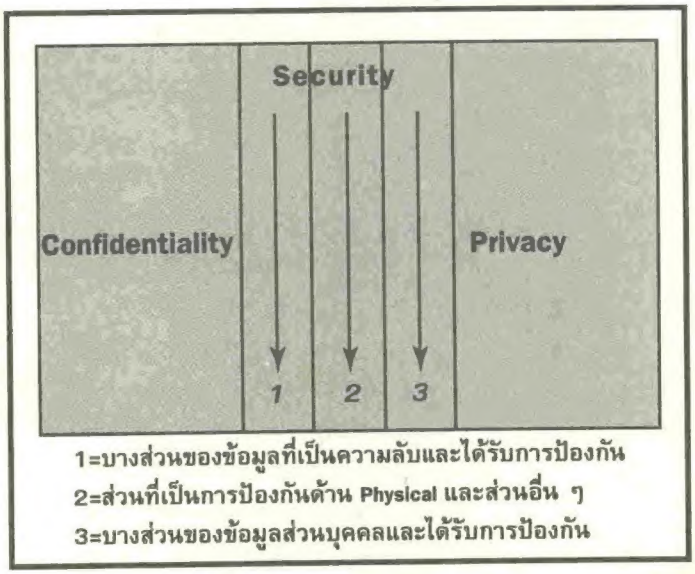
สำหรับการเก็บข้อมูลด้านบุคคลนั้นเป็นเรื่องที่ต้องให้ความสำคัญและตระหนักถึงความปลอดภัยเป็นอย่างยิ่งไม่น้อยกว่าข้อมูลในลักษณะอื่น ๆ เพราะเราควรถือว่าบุคคลเป็นทรัยากรที่มีความสำคัญมาก เคยมีคนเปรียบเปรยไว้ว่า ถึงแม้องค์กรใดก็ตามจะมีระบบงานที่ดี มีเทคโนโลยีสารสนเทศที่เยี่ยมยอดเพียงใด หากขาดบุคลากรที่มีความรู้ ความสามารถ และที่สำคัญคือความกระตือรือร้น ขวนขวายที่จะพัฒนาตนเองอยู่เสมอแล้วล่ะก็ นั่นหมายถึงจุดจบของสารสนเทศองค์กรนั่นเอง และถ้าเรามีการบันทึกข้อมูลที่มีประสิทธิภาพแต่ไม่มีนโยบายในการรักษาความปลอดภัยของข้อมูลโดยเฉพาะอย่างยิ่งข้อมูลบุคคล ก็อาจจะนำความเสียหายมาสู่องค์กรได้

ข้อมูลบุคคลที่กล่าวถึงนี้ เมื่อพิจารณาดูแล้วจะพบว่ามีข้อมูลอยู่หลายประเภท เราลองมาแบ่งแยกกันดูนะครับว่ามีอะไรบ้าง

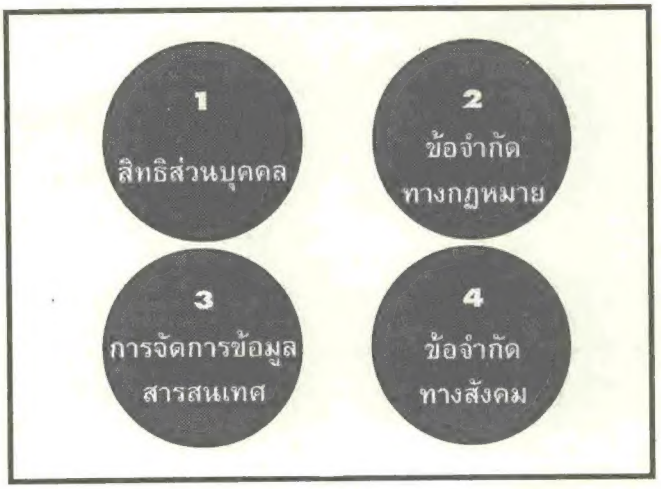
1. ข้อมูลบุคคล
2. ข้อมูลการติดต่อ
3. ข้อมูลการศึกษา
4. ข้อมูลการทำงาน
5. ข้อมูลความสามารถพิเศษ
6. ข้อมูลใบอนุญาตต่าง ๆ
7. ข้อมูลสุขภาพและการรักษาพยาบาล
8. ข้อมูลเงินเดือน
9. ฯลฯ

ข้อมูลที่ลองแบ่งแยกออกมาข้างต้นนั้น ถึงแม้ว่าจะดูแล้วรู้สึกว่าธรรมดา แต่ในปัจจุบันนี้กลับกลายเป็นประเด็นที่เป็นข้อถกเถียงกันอยู่ในการที่จะต้องคอยตรวจสอบในการบันทึกข้อมูล ประเด็นที่ผมกำลังจะกล่าวถึงนี้คือ

1) เรื่องสิทธิส่วนบุคคล
2) เรื่องการจัดการข้อมูลสารสนเทศ
3) เรื่องข้อจำกัดทางกฎหมาย
4) เรื่องข้อจำกัดทางสังคม (ดังรูปที่ 2)



รูปที่ 1
ลำดับความเกี่ยวข้องของข้อมูลทางบุคลากร



รูปที่ 2
ประเด็นที่ควรให้ความสำคัญของข้อมูลทางบุคลากร

1. สิทธิส่วนบุคคล เนื่องจากระบบคอมพิวเตอร์มีประโยชน์ในการบันทึกข้อมูลและการไหลเวียนของข้อมูลทำให้ง่ายต่อการกำหนดรายการต่าง ๆ การรวบรวมข้อมูลตลอดจนการกระจายข่าวสารไปในทุก ๆ ระดับขององค์กรเจ้าของข้อมูล (หมายถึงเจ้าหน้าที่ในองค์กร) ควรจะได้รับความคุ้มครองและสิทธิในการเลือกปฏิบัติโดยไม่ถูกควบคุม เช่น ให้สิทธิพนักงานเลือกว่าจะไม่ต้องการให้พิมพ์ที่อยู่และเบอร์โทรศัพท์ ข้อมูลทางการแพทย์ เป็นต้น โดยทางบริษัทอาจจะใช้การออกแบบระบบสารสนเทศในการช่วยกำหนดขอบเขตความปลอดภัย รวมทั้งนโยบายรักษาสิทธิประโยชน์ส่วนบุคคลของเจ้าหน้าที่มาเป็นเครื่องมือเพื่อคุ้มครองและรักษาสิทธิของเจ้าหน้าที่ เว้นแต่ความยินยอมเป็นรายบุคคลเท่านั้น

2. การจัดการข้อมูลสารสนเทศ ธุรกิจโดยทั่วไปมักต้องการจะไม่เปิดเผยข้อมูลกิจการของตนต่อสาธารณชน เนื่องจากเหตุผลในด้านของการแข่งขัน ไม่ต้องการคู่แข่งทราบถึงการดำเนินการบริหารของกิจการตน แต่เมื่อมีความต้องการข้อมูลเพื่อใช้ในการตัดสินใจแล้วก็ควรมีการกำหนดวิธีการที่จะนำข้อมูลออกมาอย่างถูกต้อง ถูกระเบียบ โดยได้รับความคุ้มครองหรืออยู่ภายใต้ระบบรักษาความปลอดภัย ดังนั้นในการนำเครื่องมืออัตโนมัติต่าง ๆ มาใช้ก็เพื่อจัดการเรื่องข้อมูลข่าวสารให้ดีขึ้น โดยจำเป็นต้องมีระบบป้องกันทั้งข้อมูลในเครื่องและควบคุมในเรื่องการออกรายงานต่าง ๆ ด้วย

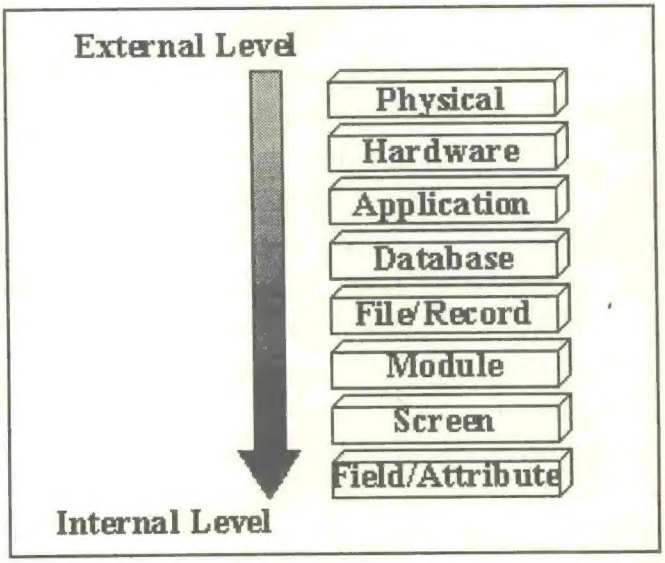
3. ข้อจำกัดทางกฎหมาย ฝ่ายทรัพยากรบุคคลควรคำนึงถึงสิ่งที่เป็นความต้องการของรัฐในเรื่องของสิ่งที่รัฐต้องการกับข้อมูลที่มีลักษณะเป็นสิทธิส่วนบุคคล ซึ่งก็ควรให้ความสำคัญและพิจารณาด้วยว่าข้อมูลใดที่จำเป็นใช้สำหรับการนำส่งต่อหน่วยงานรัฐบาล ข้อมูลใดที่เป็นข้อมูลส่วนบุคคล เช่น การจัดทำรายงานอัตรากำลังที่ต้องรายงานต่อแรงงานจังหวัดในกรณีที่เป็นกิจการประเภทการผลิต เป็นต้น ก็มีความจำเป็นที่ต้องแจ้งให้พนักงานทราบและมีการปฏิบัติอย่างรัดกุมในการนำข้อมูลไปใช้

4. ข้อจำกัดทางสังคม ประเด็นสุดท้ายที่ควรคำนึงถึงคือข้อมูลส่วนบุคคลที่มีผลต่อสังคม สังคมในที่นี้รวมถึงสังคมครอบครัว สังคมการทำงาน สังคมเพื่อนด้วย ข้อมูลเหล่านั้น เช่น ข้อมูลเกี่ยวกับโรคติดต่อ ข้อมูลสถานภาพสมรส (โสด หย่าร้าง แยกกันอยู่) เป็นต้น

การป้องกันข้อมูล

ในการเปิดเข้าสู่ข้อมูลผู้ใช้ต้องพิจารณาถึงการป้องกันทางกายภาพเป็นอย่างแรก ไม่ว่าจะเป็นการทำงานอยู่บนระบบเครือข่ายหรือเครื่องคอมพิวเตอร์สำหรับผู้ใช้เครื่องเพียงคนเดียว (a single-user) ก็จำเป็นต้องมีการป้องกัน เช่น การป้องกันทางกายภาพ (Physical) โดยใช้การ log on hard drive หรือ log your office, การป้องกันทาง (Logical) โดยการใช้ password เป็นต้น การป้องกันที่ง่ายที่สุดเมื่อใช้งานเพียงคนเดียว คือการใช้โปรแกรม Screen-saver จะช่วยป้องกันไม่ให้คนอื่นรู้ว่าสิ่งที่เรากำลังทำอยู่นั้นคืออะไร ต้องใช้ password ในการติดต่อใช้งานก็เป็นอีกวิธีหนึ่งที่ช่วยป้องกันได้ผลในระดับเบื้องต้น และการใช้เครื่องมือทางซอฟต์แวร์ (Tool) ในการสร้างระดับของผู้ใช้งาน (Accessible Security) ไม่ให้เข้าไปในข้อมูลที่ได้ป้องกันไว้ (ดังรูปที่ 3)

ดังนั้นการเข้าสู่ระบบการบันทึกข้อมูลบุคคลควรจะเริ่มต้นด้วยการมี password สำหรับการ log-in และการป้องกันดังกล่าวด้วย password เป็นเพียงระดับแรก ๆ ของการ



รูปที่ 3
ลำดับขั้นการป้องกันข้อมูลทางบุคลากร

ป้องกันเท่านั้น เพราะการกำหนดค่าของระบบความปลอดภัยตั้งแต่อย่างง่ายไปจนกระทั่งชนิดที่มีความซับซ้อน ซึ่งขึ้นอยู่กับการนำข้อมูลไปใช้ เช่น การติดตามผู้สมัครงานและงานด้านฝึกอบรม การกระจายข่าวสาร ข้อมูลเกี่ยวกับวิธีการทำงาน เป็นต้น จะมีค่าระดับความปลอดภัยต่ำ เพราะข้อมูลไม่ใช่เรื่องที่พึงระวังมากเหมือนเรื่องของการวางแผนความสำเร็จในงาน (Succession Planning) การวางแผนอัตรากำลัง (Manpower Planning) การประเมินผลเพื่อการปรับเงินเดือน (Evaluation) ซึ่งจะถูกออกแบบให้มีค่าระดับความปลอดภัยที่สูง เนื่องจากเป็นความลับพนักงานและองค์กร หากมีการเผยแพร่ออกไปอาจเกิดการเปรียบเทียบและเกิดความขัดแย้งภายในองค์กร (Conflict) ในที่สุด

ในการเพิ่มประสิทธิภาพของระบบความปลอดภัยองค์กรควรจัดโครงสร้างของผู้มีอำนาจใช้งานให้ชัดเจน โดยการกำหนดว่าผู้ใช้แต่ละคนที่จะเข้าสู่ข้อมูลนั้น ๆ ได้หรือไม่อย่างไร มีอำนาจใช้งานในขอบเขตใด อาจจะมีสิทธิเข้าไปเรียกดูข้อมูลได้ในบางอย่าง แต่ไม่ได้หมายถึงทุกโปรแกรม ซึ่งอาจจะสามารถเรียกใช้ไฟล์ต่าง ๆ ที่มีอยู่ในการอ่านอย่างเดียว (Read Only) แต่ไม่ได้รับอนุญาตให้แก้ไขข้อมูลได้ (Update) ในบางกรณีอาจจะมีหน้าที่ในการหาป้อนข้อมูล (Input) เข้าเครื่องได้แต่ไม่สามารถอ่านได้ว่ามันไปอยู่ที่ใด ซึ่งถือว่าเป็นการป้องกันช่วยทำให้ข้อมูลไม่รั่วไหลได้ในระดับหนึ่ง

การป้องกันข้อมูลในระดับบุคคล

การรักษาความปลอดภัยในที่นี้ควรใส่ใจในทุกเรื่อง ไม่ว่าจะเป็นการป้องกันการเข้าไปใช้คอมพิวเตอร์เท่านั้น ต้องรวมถึงอุปกรณ์ ซอฟต์แวร์ การเชื่อมโยงระบบ ฯลฯ เนื่องจากการลักลอบขโมยหรือทำลายข้อมูลนั้นมีเทคนิคหรือขั้นตอนการเรียกใช้ข้อมูลซึ่งเรามิอาจคาดเดาเองได้ จึงควรเตรียมป้องกันให้พร้อมอยู่เสมอในทุก ๆ เรื่อง แต่ก็อย่าลืมว่า การป้องกัน

ที่มากเกินไปก็เหมือนกับไม่มีการป้องกันเลย เพราะจะไม่มีใครอยากใช้ข้อมูล เนื่องจากการเข้าถึงระบบเป็นเรื่องที่ทำได้ยาก ดังนั้นผู้ที่มีส่วนเกี่ยวข้องในการออกแบบระบบรักษาความปลอดภัยของการเก็บบันทึกข้อมูลควรจะนึกถึงประโยคที่ว่า "ความพอดีเป็นสิ่งสำคัญที่สุด" จึงต้องเตรียมหามาตรการป้องกันข้อมูลของพนักงานไม่ให้เกิดการรั่วไหล ข้อมูลบุคคลถือว่าเป็นความลับขององค์กรและเป็นสิทธิส่วนบุคคลอย่างหนึ่ง ดังนั้นจึงควรมีการควบคุมการเข้าไปใช้ข้อมูลของผู้มีหน้าที่เกี่ยวข้อง ไม่ว่าจะเป็นเจ้าหน้าที่จัดฝึกอบรม ฝ่ายสวัสดิการและเงินเดือน ฯลฯ โดยพัฒนาออกแบบโครงสร้างอำนาจในการเปิดใช้ข้อมูลซึ่งให้สิทธิในการใช้แก่ผู้ใช้ในระดับต่าง ๆ ในปริมาณงานที่ไม่เท่ากัน เมื่อมีเจ้าหน้าที่เข้ามาใหม่ควรจะมีการสรุปย่อให้ผู้มาใหม่ได้รับทราบขั้นตอนในการบันทึกข้อมูลตลอดจนข้อควรปฏิบัติในการรักษาความปลอดภัยของข้อมูล เพื่อให้เข้าใจและจะได้ทำงานได้ถูกต้อง

นอกจากนั้น เมื่อมีการนำระบบป้องกันชนิดใหม่เข้ามา พนักงานทุกคนควรจะเรียนรู้และศึกษาให้เข้าใจทำงานในระบบได้อย่างมีประสิทธิภาพ โดยก่อนหน้านี้ผู้ดูแลรับผิดชอบระบบงานและผู้ขาย ควรทำงานร่วมกันเพื่อใช้การกำหนดค่าระบบความปลอดภัยให้เกิดประโยชน์สูงสุด ศึกษาว่าผู้ใช้ระดับใดสามารถใช้ข้อมูลได้เพียงใด โดยต้องพิจารณานโยบายของบริษัทด้วย

การป้องกันข้อมูลในระดับองค์กร

ในการบริหารจัดการวางแผนความปลอดภัยในการบันทึกข้อมูลบุคคลขององค์กร ผู้บริหารและผู้จัดการระบบสารสนเทศทางการบริการทรัพยากรบุคคล ควรผสมผสานรูปแบบการควบคุมหลาย ๆ วิธี ตั้งแต่วิธีที่ง่ายที่สุดไปจนถึงวิธีการที่มีความยุ่งยากซับซ้อน ทั้งการสำรองข้อมูล การดำเนินการใช้รหัสผ่าน เพราะข้อมูลฝ่ายบุคคลมักจะเป็นความลับ เมื่อใดก็ตามที่เจ้าหน้าที่ผู้รับผิดชอบในการพัฒนาระบบนั้น ๆ เกิดปัญหาขัดแย้งกับบริษัทและลาออกไปก็จะเป็นเรื่องที่น่ากลัวมาก เพราะอาจมีการทำลายหรือแปรเปลี่ยนระบบงานนั้นให้ใช้งานไม่ได้ จึงควรป้องกันข้อมูลไว้หลาย ๆ วิธี ทางแก้ที่ดีวิธีหนึ่ง ก็คือ ต้องสร้างจิตสำนึกให้เจ้าหน้าที่เหล่านั้น มีความรักและความซื่อสัตย์ต่อหน่วยงานและการจัดทำเอกสาร System document ของระบบงานนั้น ๆ ไว้เป็นอย่างดีทุกครั้ง เมื่อมีการแก้ไขเปลี่ยนแปลงระบบงานก็มีการปรับแก้ให้ตรงตามระบบงานที่แก้ไขและจัดเก็บเอกสารไว้อย่างปลอดภัย

ดังนั้น เมื่อมีเวลาว่างต้องหมั่นตรวจสอบทำนุบำรุงและพัฒนาระบบความปลอดภัยอย่างสม่ำเสมอ เพื่อหามาตรการป้องกันการสูญเสียข้อมูลทั้งจากอุบัติเหตุและจากความตั้งใจ โดยอาจจะศึกษาหาข้อมูลเพิ่มจากการศึกษาหนังสือคอมพิวเตอร์ ข่าวเกี่ยวกับ IT หรือถามจากผู้ชำนาญที่มีประสบการณ์สูง จะทำให้ทราบวิธีการในการป้องกันแบบใหม่ ๆ เช่น การจัดเก็บข้อมูลลงบน "Raid Disk" เป็นต้น ในขณะที่มีผู้คิดหาทางป้องกัน ก็มักจะมีผู้คิดหาทางทำลายอยู่เสมอ ดังนั้นจึงไม่อาจจะบอกได้ว่ามีระบบการป้องกันความปลอดภัยของข้อมูลได้สมบูรณ์แบบร้อยเปอร์เซ็นต์

สำหรับการเลือกระบบความปลอดภัยในการเก็บรักษาข้อมูลเข้ามาใช้นั้น องค์กรควรไตร่ตรองว่า ขอบเขตแค่ไหนจึงจะพอสำหรับองค์กรในการใช้งาน สิ่งต่าง ๆ ที่ควรคำนึงได้แก่

1. จะป้องกันอะไร ข้อมูลในระดับไหนที่จำเป็นจะต้องเก็บไว้อย่างดี ข้อมูลส่วนไหนที่ไม่คุ้มที่จะเสียทรัพยากรไปกับการป้องกัน ในส่วนนี้มักจะเป็นการป้องกันในเรื่องอื่น ๆ ที่ไม่เกี่ยวข้องกับคน เช่น ภัยธรรมชาติ เป็นต้น

2. จะป้องกันจากใคร ถ้าต้องการป้องกันจากบุคคลภายนอกก็อาจจะต้องใช้การเข้ารหัสข้อมูลและเพิ่มการควบคุมการเข้าถึงเครื่อง แต่ถ้าเป็นการป้องกันจากบุคคลภายในแล้ว การใช้ password ก็ถือว่าเป็นเครื่องมือที่ใช้ได้ดีแล้วในบางครั้งการป้องกันจากบุคคลภายนอกและบุคคลภายในยังไม่เพียงพอ ซึ่งควรจะระมัดระวังความผิดพลาดที่เกิดขึ้นจากผู้ใช้งานด้วย (Human Error)

3. ทรัพยากรที่จะใช้ไปกับระบบรักษาความปลอดภัยคุ้มค่าหรือไม่ เมื่อเทียบกับความเสียหายที่อาจเกิดขึ้นหากไม่มีการป้องกัน เช่น ต้องมีการใช้เทคโนโลยีที่ทันสมัยมาก ๆ หรือไม่เพื่อป้องกันข้อมูลบุคคลของบริษัท แต่ถ้าเป็นการป้องกันข้อมูลประวัติอาชญากร ก็อาจจำเป็นและคุ้มค่าที่จะลงทุน เป็นต้น

แนวทางสนับสนุนให้มีข้อมูลความปลอดภัยอีกประการหนึ่งที่มีประโยชน์มากก็คือ มาตรการคุ้มครองความปลอดภัยในเรื่องข้อมูลที่เป็นสิทธิส่วนบุคคล เหมือนอย่างในประเทศสหรัฐอเมริกาที่มี Privacy Act ซึ่งประกาศใช้ตั้งแต่ปี ค.ศ. 1974 ให้ความคุ้มครองเรื่องข้อมูลสิทธิส่วนบุคคล ดังนั้น จึงควรจะตื่นตัวกันตระหนักในความสำคัญของความปลอดภัยในข้อมูล มิให้ผู้อื่นลักลอบไปใช้ทำธุรกิจ เช่น แอบเอาข้อมูลชื่อที่อยู่ไป แล้วส่งจดหมายเชิญชวนซื้อของหรือให้ใช้บริการต่าง ๆ ในรูปแบบของการทำธุรกิจ เป็นต้น ซึ่งพบบ่อยครั้งมากที่มีผู้ทำพฤติกรรมเช่นนี้

สรุป

ผู้ที่รับผิดชอบงานด้านบุคคลควรจะตระหนักถึงความสำคัญของความปลอดภัยในการบันทึกข้อมูลบุคคล หาทางป้องกันรักษาความปลอดภัยแก่ข้อมูล เพื่อมิให้มีการปอนข้อมูลหรือทำลายข้อมูล จึงจำเป็นต้องมีมาตรการในการควบคุมการเปิดเข้าไปใช้งานในระบบสารสนเทศทางการบริหารทรัพยากรบุคคล เช่น การใช้รหัสของผู้ใช้ (User-ID) การป้องกันมิให้ผู้ใช้บันทึกข้อมูลอันใดเข้าไปเพิ่มได้ การทำสำเนาข้อมูลสำรองเพื่อป้องกันความเสียหายที่อาจเกิดจากสื่อบันทึกข้อมูลหรือภัยพิบัติต่าง ๆ เป็นต้น

นอกจากนี้ การพัฒนาระบบสารสนเทศทางการบริหารทรัพยากรบุคคล ผู้ชำนาญการทางด้านบุคคล และผู้ชำนาญการทางด้านสารสนเทศระบบงาน ควรวางแผนออกแบบระบบร่วมกัน โดยคำนึงถึงเรื่องข้อมูลสิทธิส่วนบุคคล เพื่อกำหนดรูปแบบควบคุมให้เปิดเข้าไปได้เฉพาะบุคคลที่ได้รับอนุญาตภายใต้เงื่อนไขที่ควบคุม ระบบในการจัดการข้อมูลสารสนเทศและข้อจำกัดต่าง ๆ ทางกฎหมายและทางสังคมที่เกี่ยวข้องกับการดำเนินงาน หากมีความปลอดภัยของข้อมูลมากเท่าใด ก็จะทำให้ระบบงานต่าง ๆ ทำงานได้อย่างมีประสิทธิภาพยิ่งขึ้น

จะเห็นได้ว่าความสะดวกสบายที่มนุษย์ได้รับนั้น มิใช่ขึ้นอยู่กับเทคโนโลยีสารสนเทศเท่านั้น หากแต่ขึ้นอยู่กับความปลอดภัยของสารสนเทศด้วย หวังว่าในอนาคตอันใกล้ องค์กรต่าง ๆ จะตระหนักถึงความสำคัญของความปลอดภัยของข้อมูลมากขึ้นในทุก ๆ ด้าน ไม่เฉพาะแต่ในด้านบุคคลเท่านั้น แต่รวมถึงความเคารพในเรื่องสิทธิส่วนบุคคลของผู้อื่นด้วย

หมายเหตุ

[1] Parker, D.B. (1981.) Computer Security Management. Virginia: Reston Publishing Company , Inc.

[2] Torrington, D.& Hall, L. (1995). Personnel Management : HRM in Action. (3rd ed.). UK : Prentice Hall International Limited.

[3] Ceriello, V.R.& Freeman, M.C. (1991). Human Resource Management Systems : Strategies, Tactics, and Techniques. New York : Lexington Books, pp. 105.